IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF J. ALEX HALDERMAN IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

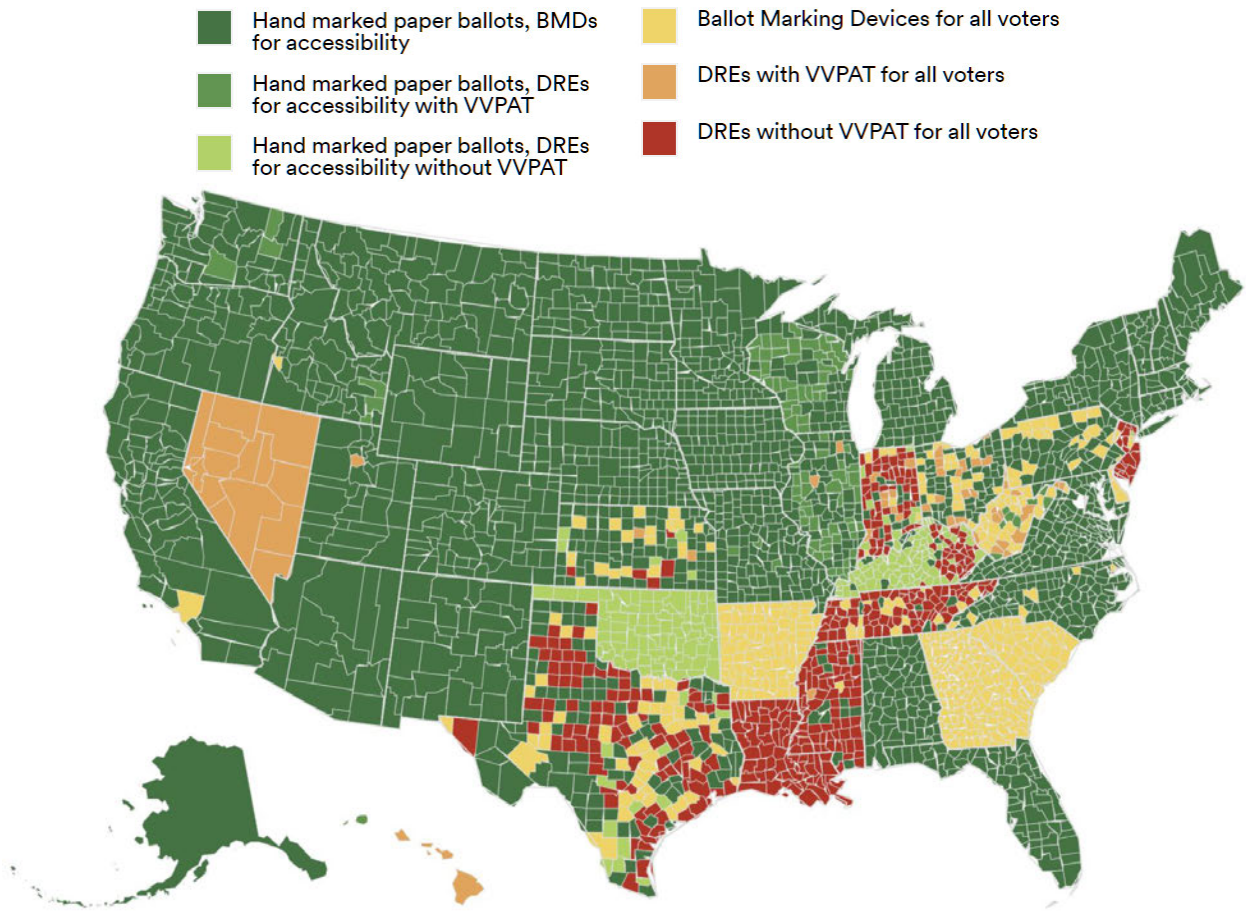
2. State Defendants characterize Georgia's BMD-based election system as "an electronic voting system used throughout the country,"[1] and they remark that BMDs are used in "six of the ten largest counties in the country, including Los Angeles, California; Cook County/City of Chicago; Maricopa, Arizona; San Diego,

[1] State Defendants' Response in Opposition to Curling Plaintiffs' Fourth Motion for Preliminary Injunction, Dckt. 821 at 1.

California; Dallas, Texas; and Riverside, California."[2] These statements are misleading. The vast majority of jurisdictions that use BMDs use hand-marked paper ballots as the primary method of voting and reserve BMDs for accessibility purposes—including four of the six localities that State Defendants cite (all but Los Angeles and Dallas).[3] I explained in my previous declaration that BMDs are much safer when used by only a small fraction of voters, as in these localities.[4]

3. The map below shows the primary in-person voting technology that will be used in each U.S. county this November. The great majority of states, counties, and voters will use hand-marked paper ballots with BMDs available for accessibility (shown in dark green).

[2] *Id*. at 19.
[3] Verified Voting, *The Verifier*, https://verifiedvoting.org/verifier/ (accessed Aug. 30, 2020.)
[4] Decl. of J. Alex Halderman (Aug. 19, 2020), Dckt. 785-2 at 47-50.



Primary Polling-Place Equipment by County, November 2020

(Data/image: Verified Voting, *The Verifier*, https://verifiedvoting.org/verifier/.)

4. State Defendants further characterize Georgia's BMD-based election system as "a system recommended by the National Academy of Sciences and the U.S. [*sic*.] Intelligence Committee."[5] Again, this statement is misleading. Both the

[5] Dckt. 821 at 1.

National Academies[6] and the Senate Select Committee on Intelligence[7] recommended the use of voter-verified paper ballots, as opposed to paperless DREs or DREs with VVPAT printers. These recommendations were based on testimony heard in 2017 and 2018, including my own testimony to each body. At the time, only about 1% of voters lived in jurisdictions with BMDs as the primary method of voting, while nearly a quarter of voters used paperless DREs. Moreover, there had been little research about whether BMD ballots were accurately verified by voters. An election system like Georgia's, which uses barcode-based BMDs for nearly all in-person voters statewide, was not specifically addressed in either report.

---

[6] National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* (2018) at 80, available at http://nap.edu/25120. "Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine (using a ballot-marking device); they may be counted by hand or by machine (using an optical scanner). […] Voting machines that do not provide the capacity for independent auditing (e.g., machines that do not produce a voter-verifiable paper audit trail) should be removed from service as soon as possible."

[7] U.S. Senate Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure" (June 2019) at 59, available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf. "As states look to replace HAVA-era machines that are now out of date, they should purchase more secure voting machines. Paper ballots and optical scanners are the least vulnerable to cyber attack; at minimum, any machine purchased going forward should have a voter-verified paper trail and remove (or render inert) any wireless networking capability."

5. The Academies' 2018 report also notes that "[w]ell designed, voter-marked [i.e., marked by hand] paper ballots are the standard for usability for voters without disabilities. Research on VVPATs has shown that they are not usable/reliable for verifying that the ballot of record accurately reflects the voter's intent, but there is limited research on the usability of BMDs for this purpose. […] Additional research on ballots produced by BMDs will be necessary to understand the effectiveness of such ballots."[8] It goes on to call on the National Science Foundation and other federal agencies to fund research to "determine voter practices regarding the verification of ballot marking device–generated ballots and the likelihood of voters, both with and without disabilities, will recognize errors or omissions."[9]

6. Last year, with National Science Foundation funding, my research group conducted an extensive study on this question, which I discuss at length in a previous declaration.[10] Our study was peer reviewed and published in January 2020 at the IEEE Symposium on Security and Privacy,[11] which is the most selective top-tier

---

[8] *Securing the Vote* at 79-80.
[9] *Id*. at 124.
[10] Decl. of J. Alex Halderman, Dckt. 682 (Dec. 16, 2019) at 25-33.
[11] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" in *Proceedings of the 41st IEEE Symposium on*

publication venue for computer security research. The work received special commendation from the review committee as the best research paper with a graduate student as the first author to appear in this year's symposium. The main findings of the study were that 60% of voters failed to review their ballots at all, and voters only reported 6.6% of misprinted ballots caused by a hacked BMD. We also tested a variety of procedural interventions, including those practiced in Georgia, to see how much they improved verification, but the magnitude of the improvements was likely too small to allow election officials to reliably detect BMD attacks in close races.

7. Other recent research, which State Defendants' and their expert Dr. Gilbert cite favorably,[12] actually confirms the key results from my study. It found that although voters *who do* review BMD printouts often are able to spot errors, few voters review the printouts at all, which is corroborated by field reports from polling place observers. These findings are further bolstered by previous research in the contexts of VVPATs and DRE review screens, which found that voters are also unlikely to catch errors when using those technologies.[13]

Security and Privacy (2020), https://jhalderm.com/pub/papers/bmd-verifiability-sp20.pdf.

[12] Dckt. 821 at 11, "there is other research indicating that voters can detect manipulation of ballots."

[13] This literature is summarized in Bernhard et al., § II.B.

8. On this basis, I find it misleading for State Defendants to say that "the science is not yet settled" regarding whether voters accurately verify BMD printouts.[14] Although science is always open to new evidence, there are now several studies that strongly support the proposition that the voter population does not verify BMD printouts accurately enough to allow reliable detection of misprinting attacks. To my knowledge, there is no research at all that suggests the contrary.

9. State defendants incorrectly ascribe my technical conclusions about the relative security of different voting technologies to mere personal preference.[15] This mistakes cause for effect. Like other security experts, I generally recommend hand-marked paper ballots over DRE and all-BMD systems *because* only a primarily hand-marked system can be strongly defended in practice using existing technology. My recommendations would change as appropriate if technological breakthroughs or compelling new scientific results were to alter the security analysis.

10. State Defendants misread my earlier testimony and erroneously conclude that I have changed my views about BMD auditability: "While Dr.

---

[14] Dckt. 821 at 11.

[15] *Id*. at 17. "Dr. Halderman's opinions are based on his personal beliefs that hand-marked paper ballots are a superior election system. He simply decided, as a policy matter, that the only acceptable election system is hand-marked paper ballots and reasons backward from that conclusion."

Halderman previously agreed that a sufficient audit of a BMD-generated ballot can 'detect and correct' the kinds of hypothetical hacking attacks about which he warns, [Doc. 619-2 at ¶¶ 6-7], he now says that no audit of any BMD system would ever be enough to satisfy him, [Doc. 785-2 at ¶ 51]."[16] There is no contradiction. Both declarations discuss two styles of attack: (1) changing both the barcode and the human-readable text and (2) changing only the barcode. Both declarations explain that the first kind of attack could not be detected by any kind of audit of the printouts, since all the records of the voter's intent would be fraudulent.[17] Both declarations also explain that the second kind of attack *could* be detected with a sufficiently rigorous audit that compared the contents of the barcode to the human-readable text,[18] but, to my knowledge, Georgia has no plans to conduct such an audit.

11. State Defendants falsely claim that "the evidence demonstrates that Georgia's new BMD system is completely separate from the DRE/GEMS systems, down to hand-entry from original source documents[.]"[19] To my knowledge, the only

---

[16] Dckt. 821 at 19.
[17] Dckt. 619-2 at 12; Dckt. 785-2 at 41.
[18] Dckt. 619-2 at 6-7; Dckt. 785-2 at 31-35. I was slightly imprecise in Dckt. 619-2 when I said that a sufficiently rigorous audit could "correct" a barcode-only attack in addition to detecting it. That is only the case if the auditors are somehow able to establish that the barcodes and not the human-readable text have been manipulated, but both would be suspect in the event that the BMDs had been hacked.
[19] Dckt. 821 at 8.

"evidence" for this claim appears to come from Mr. Coomer and Dr. Gilbert, but Dr. Gilbert never examined the Georgia system, and it is unclear what personal knowledge Mr. Coomer has, as there is no evidence he has conducted or participated in an examination of the Georgia system. In any event, neither could know what the workers with access to Georgia's technology are doing day to day, such as connecting USB devices to it that were connected to the prior system or connecting components to the Internet.

12. [redacted]

[20] [redacted]

[redacted]

13. While State Defendants are correct that the "Dominion system has been the subject of penetration testing" in other states,[24] they neglect to point out that this testing revealed a slate of serious vulnerabilities that likely remain unmitigated in the Dominion hardware and software used in Georgia. My previous declaration cites the results of penetration tests commissioned by the California Secretary of State, which found that attackers could modify the Dominion software installation files and "it would be possible to inject more lethal payloads into the installers", that the anti-virus software was insufficient or non-existent, and that the BMDs had

[21] Hamilton decl.
[22] The public facing portion of the ENR system is located at https://results.enr.clarityelections.com/GA/
[23] Dckt. 723 at 15 (Throop Decl.).
[24] Dckt. 821 at 10.

vulnerabilities that "would be open to a variety of actors including a voter, a poll worker, an election official insider, and a vendor insider," among other problems.[25]

14. In the context of evidence that I discuss in my previous declarations regarding vulnerabilities in the Dominion equipment uncovered by certification testing in Texas,[26] State Defendants state incorrectly that the security problems "primarily relate to the optical scanners (ICP units), not the BMDs, which Curling Plaintiffs advocate the State continue using."[27] This is misleading. Both Texas and California found serious weaknesses impacting the BMDs, including the use of dangerously obsolete software and means by which the software could be manipulated by attackers. Both also found serious weaknesses impacting the scanners. Vulnerabilities in the BMDs are relevant to the relief that Plaintiffs' seek with respect to the use of hand-marked paper ballots, which are the only practical countermeasure to some BMD-based attacks. Vulnerabilities in the scanners are a threat to Georgia elections however the ballots are marked, and they are relevant to Plaintiffs' requested relief regarding rigorous auditing of the scanners' tallies.

---

[25] Dckt. 785-2 at 21-27.
[26] *Id*. at 19.
[27] Dckt. 821 at 8, fn. 7.

Status of Forensic Testing

15. Plaintiffs have asked me to update the Court about the status of the forensic analyses that I am performing on their behalf. My work is still in progress, but there are several preliminary findings I can report.

16. In December 2019, I received a copy of a forensic image created by the FBI of the server at the KSU Center for Election Systems.

17. In late July, I began a limited analysis of log files from approximately 4500 sequestered memory cards from Cobb, DeKalb, and Fulton counties to extract DRE serial numbers for statistical sampling. On August 13, 2020, shortly after the Court granted permission for a forensic examination of the memory cards, I began creating forensic images and have so far imaged around 25% of the cards.

18. On August 25, I received forensic images of the internal memory from six AccuVote-TS DREs from Athens-Clarke County. To facilitate imaging these machines, I created a software patch for the DREs' bootloader software, which a forensic technician programmed into a read-only memory chip and physically inserted into each DREs. On August 30, I received forensic images of three memory cards associated with those DREs.

19. To my knowledge, this is the first time that detailed forensic analysis of large parts of a state-wide DRE system has been conducted. Due to the scope and

complexity of the work, my analysis is necessarily still in an initial phase. I have had to developed specialized software and techniques to efficiently image and analyze the thousands of memory cards and the proprietary data formats of the DRE system.

20. The objective of my analysis is to determine the security posture of the DRE-based system as it was operated in Georgia. Although older and newer versions of the AccuVote DRE software have been shown to suffer from critical exploitable vulnerabilities, forensic analysis allows for direct confirmation that vulnerabilities were present in the specific hardware and software configuration Georgia used. The analysis also allows me to more fully assess what opportunities attackers would have had to spread malware through the Georgia system and manipulate election results.

21. As a secondary objective, the analysis may also uncover evidence that the election system was successfully compromised. However, one of the key deficiencies of paperless voting systems is that successful attacks might not leave forensic evidence, since well designed malware would remove the electronic records of its presence once its task was complete. Although there is a possibility that attackers were careless and did leave some digital traces, absence of evidence cannot support a strong conclusion that the system was not attacked.

22. Moreover, the digital records to which Plaintiffs have access are badly incomplete. Thus far, they have received memory cards from only three counties,

and most of these cards have records from only a single election. Only six DREs have been imaged, all from a single county. Log files from the CES server from before November 10, 2016 were erased prior to the server begin imaged by the FBI, severely limiting forensic visibility into the period of Russia's documented attacks against state election systems in the leadup to the 2016 election.[28] While these data sources provide abundant insight into how the DRE-based system was operated and ways in which it was vulnerable, finding a "smoking gun" proving that a Georgia election result was stolen by hackers is akin to finding the proverbial needle in a haystack, even assuming it occurred and left some trace in the data.

23. Nevertheless, there is evidence that hackers penetrated the system. My initial analysis of the CES server image has confirmed the principal findings that Logan Lamb described in his January 16, 2020 declaration.[29] The most important finding is that the CES server likely was compromised by an external attacker in December 2014. Mr. Lamb describes this evidence in detail.[30] Determining what actions the outside party took on the server is difficult, given the amount of time that elapsed before the server was imaged, but my analysis is ongoing.

---

[28] Suppl. Decl. of Logan Lamb, Dckt. 699-10 at 21-23.
[29] *Id*. at 11.
[30] *Id*. at 13-20.

24. Even if nothing more can be determined about the apparent attack, the evidence shows that the CES server was vulnerable to unauthorized access from the Internet for many years. Additionally, the FBI image shows that the CES server housed security-critical data, including installation files for the BallotStation software that ran on every DRE, the hash verification software that CES ran on its GEMS servers, and election databases. An outside attacker who infiltrated the server and compromised these files could have spread malicious software to the GEMS servers and DREs.

25. My initial analysis of the AccuVote-TS memory images confirms several severe vulnerabilities in the DREs themselves.

26. The bootloader software used in the DREs is version 1.0.2 and dates from June 2002. This software is critical to the DREs' security, since it runs every time they are powered on and controls sensitive operations such as loading the operating system and installing software updates. That it was not updated for 18 years demonstrates that Georgia's DRE systems were subject to an even wider range of vulnerabilities than had been previously established.

27. The version of the BallotStation election software installed on the DREs is 4.5.2!, which displays a 2004 copyright date. This confirms that the Georgia BallotStation software was not materially updated since that time.

28. The installed BallotStation software matches the contents of the installer file "BS_CE-TSR6-4-5-2!-DS.ins" found on CES's Internet-facing server. This is consistent with the assertion that copies of the software to be installed on the DREs were stored on the vulnerable CES server, where they could have been modified by an attacker. Although I have thus far been unable to determine whether the installation files on the server were modified by attackers, they had the opportunity to do so.

29. By analyzing the bootloader and BallotStation software, I have so far been able to confirm the presence of several critical vulnerabilities.

a) The vulnerability discovered by Harri Hursti in 2006 and described by Michael Shamos as "one of the most severe security flaws ever discovered in a voting system" is present in the DREs software that was used in Georgia until this year.

b) The vulnerabilities I exploited in a 2007 study to create vote-stealing malware that spreads from machine-to-machine as a computer virus[31] is present in the DREs software that was used in Georgia until this year.

[31] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, "Security Analysis of the Diebold AccuVote-TS Voting Machine," in *Proc. USENIX/ACCURATE Electronic Voting Technology Workshop* (2007).

c) The vulnerability I exploited to demonstrate a vote-stealing attack to the Court in 2018 is present in the DREs software that was used in Georgia until this year.

30. All the memory cards and DREs I have analyzed use the same encryption key, `F2654hD4`. This is the default encryption key that was installed on the AccuVote DREs at the factory. It was publicly revealed by security researchers in 2003.[32]

31. Changing the encryption key to a different, secret value would have been straightforward for the state, but Georgia instead continued to use the manufacturer's default key for 17 years after that key was leaked to the public. Since the key was publicly known during that period, all confidentiality and integrity protections provided by the cryptography were completely negated. For instance, anyone with access to the memory cards could have read or modified any of the election data they contained.

32. The election log files from the county memory cards record that those cards were used in 1945 separate DREs in Cobb County, 1982 in DeKalb County,

---

[32] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, "Analysis of an Electronic Voting System," in *IEEE Symposium on Security and Privacy* (2004), § 4.4. Available at https://avirubin.com/vote.pdf.

and 2123 in Fulton County. Analysis of the logs shows that all three counties engaged in practices that would have facilitated spreading viral malware throughout their election systems.

a) County workers sometimes reused the same card in hundreds of machines for testing and training purposes. For example, in DeKalb, one memory card was sequentially inserted into at least 288 DREs. If any of those DREs was infected with viral malware, the malware could have spread to the other DREs during this operation by exploiting the confirmed vulnerabilities I discuss above.

b) In each of Fulton and Cobb counties, a single DRE was used to process data from more than a thousand different cards. If that DRE was infected with malware, it could have spread directly to over a thousand other DREs.

c) Each county used only a small number of DREs to program memory cards from the GEMS server. In Fulton, every election represented in the log files was prepared using one of only 17 machines; in Cobb, 28 machines; and in DeKalb, 28 machines. These DREs would provide a centralized point from which to launch an attack. If they were infected

with malware, the malware could have spread directly to all other DREs in the counties.

33. Despite the assertion that Georgia operated a uniform voting system across all counties, the three counties represented in my analysis had starkly different practices for maintaining their memory cards. This indicates that counties developed their own *ad hoc* processes for important security tasks. Some of these county-specific processes would have further facilitated the spread of malware.

d) Although Fulton and DeKalb counties appear to have erased their cards before each election, Cobb County did not, and some cards I examined contained election data from as long ago as 2004. This failure to erase the cards means that if they were infected, malware could continue to spread to new machines for many election cycles.

e) DeKalb County appears to have erased cards by overwriting them with the contents of other cards—most likely by using a machine designed for duplicating the cards. Around 8% of the DeKalb cards I have analyzed so far are identical to other DeKalb cards. This practice could rapidly spread malware if the cards used as a source for the duplication were infected.

34. The log files from the memory cards record hundreds of instances of technical malfunctions, including data corruption, software crashes, and machines freezing and needing to be restarted during voting. There also appear to be frequent instances of human error and procedural deviation, such as failing to correctly perform logic and accuracy testing.

35. These findings directly confirm the vulnerability of the DRE system and reveal additional ways that malware could have spread through it, beyond those already in evidence. Since my analysis is still in an early stage, it is likely that additional problems will be uncovered as the work proceeds.

Rebuttal of Declaration of Jack Cobb[33]

36. Mr. Cobb gives only a partial history of certification tests that apply to Georgia's Dominion equipment.[34] His company, Pro V&V, appears never to have performed penetration testing on the Dominion equipment nor any security testing on the version of the Dominion system used in Georgia (5.5A). Although he states that his company performed certification tests for the U.S. Election Assistance Commission ("EAC") for version 5.5 of the software, EAC certification testing

[33] Decl. of Jack Cobb (Aug. 25, 2020), Dckt. 821-6.
[34] *Id*. at 5.

involves only limited security evaluation and not penetration testing. I find it interesting that Mr. Cobb points to security tests performed by another company, SLI Compliance, as part of certification testing for Pennsylvania, but that he neglects to point to later tests performed by the same company for California, which found a number of serious vulnerabilities.[35] I discuss these vulnerabilities and their impact in my previous declaration.[36] I also find it interesting that despite the fact that Pro V&V had never performed penetration testing of the Dominion system, the Secretary of State hired Pro V&V to perform certification tests for the State of Georgia.[37]

37. In reference to my August 19, 2020, declaration, Mr. Cobb opines that I "clearly [do] not understand the specific setup and nature of the Dominion system or its security features."[38] His first example concerns the QR codes (barcodes) printed on the BMD ballots. Based on his company's role in certifying the Dominion system for the EAC and the State of Georgia, I would expect Mr. Cobb to have a detailed technical understanding of these barcodes, which are central to the security

---

[35] California Secretary of State's Office of Voting Systems Technology Assessment, "Dominion Voting Systems Democracy Suite 5.10 Staff Report" (Aug. 19, 2019) at 29, https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510staff-report.pdf.
[36] Decl. of J. Alex Halderman (Aug. 19, 2020), Dckt. 785-2 at 21-27.
[37] Cobb decl. at 6.
[38] *Id*. at 9.

of votes cast using Dominion BMDs. Indeed, Mr. Cobb states that during the limited testing that his company conducted for the Secretary of State, "Pro V&V also verified the contents of the QR code which includes a digital signature and is encrypted."[39] He later states that, "In this system, the election files, including the QR codes, are digitally signed and encrypted."[40]

38. These technical claims about the Dominion QR codes used in Georgia are entirely wrong. Based on my own analysis of the QR codes from ballot images provided by Fayette County during discovery, which I understand to be scans of ballots cast during the June 9, 2020 election, no portion of the QR codes is encrypted.[41] I am prepared to demonstrate that the contents can be read and understood without the use of a secret key, thus proving they are not encrypted.

39. Moreover, Dominion QR codes do not include a digital signature, but rather what is known as a message authentication code ("MAC"). A MAC provides

---

[39] *Id*. at 6.
[40] *Id*. at 9.
[41] In my previous declaration, I myself incorrectly described the QR codes as "encrypted" (Dckt. 785-2 at 7(a), 32). My understanding at the time, before I had received a Georgia BMD ballot with which to conduct my own tests, was based on the California Secretary of State's test report. California Secretary of State's Office of Voting Systems Technology Assessment, "Dominion Voting Systems Democracy Suite 5.10 Staff Report" (Aug. 19, 2019): "The QR code is encrypted" (p. 14); "The ICX ballot marking device uses an encrypted QR code" (p. 28).

somewhat similar protections to a digital signature but is weaker in important aspects. The distinction between digital signatures and MACs is an elem-entary concept that I regularly test students about in introductory security classes.

40. Mr. Cobb's errors about these basic facts regarding the Dominion system and its security are troubling. They lead me to believe either that Mr. Cobb does not understand the specific setup and nature of the Dominion system or its security features, that he is not telling the truth when he states that his laboratory "verified the contents of the QR code" while testing the system for Georgia, or that Pro V&V's tests of critical aspects of the system were poorly conducted.

41. Mr. Cobb goes on to imply that the Dominion voting system software cannot be altered by attackers without detection, because the BMDs have "a built-in feature that will generate a SHA-256 hash value at any point before and during voting to allow for easy checks to determine if it matches with Georgia's version."[42] This view again reflects a misunderstanding of fundamental security concepts, such as what hash values are and how they can be used to verify the integrity of software.

42. In the security field, a hash value is a number that is calculated based on the contents of a file by applying an algorithm that is designed so that it is

[42] Cobb decl. at 7.

extremely difficult for an attacker to generate another file with different content that yields the same hash value. Given two files, I can apply a hash algorithm to compute the hash value of each file, and if the hash values are identical, I can conclude that the files' contents are also identical.

43. The scenario Mr. Cobb describes is completely different. Instead of Mr. Cobb calculating the hash values of the files on the BMD, he describes a scenario where the software on the BMD calculates *its own* hash value, which is then compared to the hash value of the software that is supposed to be installed—in essence, asking the BMD itself whether it is malicious. This is akin to a bouncer asking bar patrons to card themselves. If the BMD *has* been attacked and is running malicious software, that software can simply lie about its hash value.

44. Hash values are not trustworthy if the system used to compute and display them is compromised. In this case, the software running on the BMD is computing and displaying its own hash. If the software has been compromised because the machine has been infected with malware, the compromised software could display whatever hash the attacker has programmed—including the hash of the uncompromised software. This mechanism may have utility for administrative compliance (e.g., checking which version of the software is supposedly installed), but it has little or no value for deterring attacks.

45. Mr. Cobb also says his firm helped Georgia "perform acceptance testing of each BMD using a hash value. This ensured that the BMD had not been altered and had the correct software installed at the time it was accepted by the State."[43] Here, acceptance testing refers to checking the hash of the software on the machine at the time it is delivered from the manufacturer. Mr. Cobb does not specify the procedure he used to conduct these tests, but verifying the integrity of software running on an embedded device such as the ICX BMD is difficult to do securely. If there is already malware on the device, that malware can conceal its presence from other software using what is known as a rootkit. Therefore, computing hash values on the device itself is not a reliable method of acceptance testing. Nor can one simply remove the storage medium and hash it using a trusted computer, since the flash storage chips in the ICX are permanently integrated into the circuitry. In any event, Mr. Cobb only describes checking the integrity of the BMD software when the BMDs were first delivered, so this testing could not prevent the software from being altered later by attackers. Nor could it detect any subsequent attack.

46. Mr. Cobb also mistakenly concludes that "[i]f a QR code was somehow manipulated on the BMD (which I have never seen occur in any context using the

[43] *Id.* at 8.

Dominion system), the digital signature would also be altered and it would not be accepted by the scanner." Again, the QR codes do not contain a digital signature, but rather a MAC. Even then, the data protected by the MAC is the same in every ballot that has the same votes. This means, for example, that an attacker can simply duplicate the QR code from a ballot with votes he favors in order to produce another ballot with those same votes that will be accepted and counted by the scanner. This is an important security flaw that Pro V&V should have been aware of after reviewing the contents of the QR codes. Dominion could have designed the QR codes in a way that would have allowed the scanners to detect and prevent such duplication, but did not do so.

47. Mr. Cobb goes on to imply that malware cannot be spread to scanners or BMDs from the election management system ("EMS"), because "the election files, including the QR codes, are digitally signed and encrypted," and if the digital signatures do not match, "decryption fails and nothing is loaded on the machine."[44] Once again, this assertion is technically nonsensical, even aside from the fact that the QR codes are neither signed nor encrypted. Although the ballot programming that workers copy to the BMDs and scanners from the EMS may be encrypted and

[44] *Id*. at 10.

signed, this has no relevance to whether malware can spread from the EMS as part of those files. The EMS *generates* the ballot programming files. Therefore, malware running on the EMS could arbitrarily alter their contents before the encryption and signatures are applied, ensuring that the BMDs would accept the files as genuine.

48. In a similar vein, Mr. Cobb asserts that, "If a QR code was somehow manipulated on the BMD […], the digital signature would also be altered and it would not be accepted by the scanner."[45] This is, again, nonsense. First, the QR code contains a MAC rather than a digital signature. A MAC is a number that works similarly to a hash, except that its value can only be computed with knowledge of a secret key. Each QR code contains a MAC of the vote data that is computed using a secret key that is shared by the BMD and the scanner. The scanner reads the QR code, extracts the vote data and MAC, and uses the secret key to compute the correct MAC of the vote data. If the MAC from the QR code is different from the computed MAC, the scanner should reject the ballot.

49. This implies that in order to print *any* ballots that the scanner will accept, the software on the BMD must have access to the secret key. Therefore, if the BMD is infected with malware that modifies the operation of the software, the

[45] *Id*. at 11.

malware too will have access to the secret key, and will be able to generate QR codes that the scanner will accept as valid for whatever ballot choices the attacker prefers.

Rebuttal of Declarations of Juan E. Gilbert

50. State Defendants have refiled a declaration from Dr. Juan E. Gilbert November 13, 2019.[46] I respond to Dr. Gilbert's assertions in my declaration of December 16, 2019.[47]

51. In a brief supplemental declaration, Dr. Gilbert makes several additional statements that require clarification.[48]

52. Dr. Gilbert correctly notes new SEB rules require poll workers to verbally instruct voters to review their ballots.[49] As Dr. Gilbert points out, my own peer-reviewed research measured the effect of such instructions on verification and error detection rates and found them to have a small positive effect. However, even with such instructions, voters failed to detect about 86% of errors on BMD printouts (vs. 93% without instructions). As my study explains, voters would have to verify

[46] Decl. of Juan E. Gilbert, Dckt. 821-2, originally 658-3.
[47] Decl. of J. Alex Halderman (Dec. 19, 2019), Dckt. 682 at 16, 38-49.
[48] Supp. Decl. of Juan E. Gilbert, Dckt. 821-7.
[49] *Id*. at 7(A).

their ballots much more carefully than that in order to reliably detect outcome-changing fraud in close elections.

53. Dr. Gilbert also notes that SEB rules require reminding voters that a sample ballot is available to help with verification. My study suggests that voters who use a sample ballot do detect errors more reliably. However, the gain will be limited to the fraction of voters who can be induced to use a sample ballot. I am not aware of any research that shows verbal reminders are effective in this regard, and I would be surprised if they were.

54. Dr. Gilbert highlights a new SEB rule that holds that if, in any recount or audit, "a discrepancy is found between the voter's choice indicated by the printed text on the ballot and the result tabulated by the ballot scanner, the printed text shall control and be counted."[50] However, this rule does not provide an effective defense against BMD misprinting attacks. An attacker could cause a BMD to alter both the barcodes read by the scanners and the human readable text, in which case there would be no disagreement. And if there were a discrepancy between the barcodes and the human-readable ballot text, the reliably of both records would be in doubt, because either might have been altered.

---

[50] *Id*. at 7(B).

55. Dr. Gilbert cites a recent study by Byrne and Whitmore, which I also cite in my previous declaration.[51] Byrne and Whitemore's results are generally in agreement with my own BMD research (although, unlike my study, theirs has not been peer reviewed). Both studies find that few voters are likely to spot errors on BMD printouts. Of 108 participants who voted on a hacked BMD, Byrne and Whitemore report that only 17.5% detected alterations to the printout. This average includes both voters who were heavily primed to review their ballots through repeated verbal and written instructions and voters who were not. Unsurprisingly, the study finds that verification performance is much better among voters who actually examine their ballots, but the fact remains that only 23% of their subjects did so. This is further evidence that voters do not reliably detect errors on BMD printouts.

56. Dr. Gilbert questions why I "make no mention of interventions which foster higher review rates."[52] As I have discussed, the magnitude of the improvements that have been measured by these studies for practical kinds of interventions are simply too small to reliably uncover cheating in close elections.

---

[51] *Id*. at 8-11.
[52] *Id*. at 11 and 13.

57. Dr. Gilbert's assertion that barcode manipulation attacks could occur with hand-marked paper ballots defies common sense.[53] Although timing marks or the placement of vote targets could be manipulated, this kind of problem would be detected during routine logic and accuracy testing. Election workers would simply need to perform L&A testing with one ballot and flip through the remaining stack of blank ballots to verify that they are all the same.

58. Dr. Gilbert argues that BMD barcode manipulation attacks are "an unlikely avenue for a bad actor since, as other scholars have recently noted, such an attack is unlikely to go undetected in a jurisdiction conducting RLAs[.]"[54] The only scholar Dr. Gilbert cites for this proposition is Dr. Dan Wallach, who, like Dr. Gilbert, is the creator of a BMD system that use barcodes. The proposition is incorrect. While it is true that "an audit which recognizes a single inconsistent barcode/text combination would signal a significant problem", in order to find even a single inconsistency, the audit would have to sample at least one manipulated ballot *and* actually compare the barcode to the text. Georgia has announced no plans to inspect the barcodes during its intended audits. Even if it did, the proposed Georgia RLA is designed to target only a single race to be selected by the SOS every two

---

[53] *Id*. at 12.
[54] *Id*. at 12.

years. There is no assurance that it will select enough ballots to uncover barcode-based cheating in races that are not targeted. For instance, if the Democratic Presidential Preference Primary had been selected for audit statewide (as it was in Fulton county), the probability that the audit would have detected barcode-based fraud sufficient to change the outcome of another state-wide race with a 1% margin of victory would be only around 30%, and that's under the counterfactual assumption that the auditors decoded the barcodes. In elections where no RLA was conducted (as in every election but the November general election in even years), the probability would be 0%.

59. Contrary to Dr. Gilbert's repeated implications, the issue is not whether interventions can improve voter verification rates *at all*, but whether they can ensure that *sufficiently many* voters carefully review their ballots.[55] The effectiveness of verification for detecting attacks increases dramatically only when the rate of verification is high. When the rate is low, as appears to be the case based on a growing number of studies, small increases (like those my study found were achieved by instructing voters to verify their ballots) have little utility.

[55] *Id*. at 13.

60. Moreover, the security of Georgia's voting system depends on whether voters are likely to spot errors when using the actual BMDs operated by the state—not theoretical future BMDs with transparent screens like those conceived by Dr. Gilbert or hypothetical interventions that somehow raise voters' verification performance well beyond the levels measured thus far. In fact, that Dr. Gilbert sees a need for such BMDs seems to indicate that he recognizes the unreliability of the ballots generated by the BMDs used in Georgia, lest there would be no need for transparent screens.

61. Dr. Gilbert and I agree that scanners can be hacked and that rigorous RLAs are necessary.[56] However, he fails to acknowledge that BMDs, particularly when they are used as the primary method of voting, as in Georgia, create a second place, in addition to the scanners, where outcome-changing attacks could succeed, multiplying the opportunities for attackers. In the absence of rigorous audits of a kind not now contemplated in Georgia, barcodes greatly magnify this risk. Dr. Gilbert does not seem to seriously dispute either claim.

[56] *Id.* at 14.

Rebuttal of Declaration of Mark Riccobono

62. State Defendants have refiled a declaration from Mark Riccobono, president of the National Federation of the Blind, dated August 1, 2019.[57] I respond to Mr. Riccobono's assertions in my declaration of December 16, 2019.[58]

Remarks on Declaration of David Hamilton[59]

63. [redacted]

64. [redacted]

[57] Decl. of Mark Riccobono, Dckt. 821-8, originally 658-4.
[58] Decl. of J. Alex Halderman (Dec. 19, 2019), Dckt. 682 at 34-37.
[59] [redacted]
[60] [redacted]
[61] [redacted]

65. [redacted]

66. [redacted]

67. [redacted]

---

62 [redacted]

63 [redacted]

[redacted]

68. [redacted]

[redacted]

[64] As the Court noted, the "assessment of the eNet voter registration systems and database rang serious alarm bells." Dckt. 579 at 76.
[65] Dckt. 579 footnote at 74. "On July 1, 2019 the SOS took over hosting eNet's voter registration database that creates the express pollbooks, but continued its

[redacted]

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 1st day of September, 2020 in Rushland, Pennsylvania.

J. ALEX HALDERMAN

contract with PCC for licensed use of the PCC software and for PCC's maintenance and support of the PCC application."

66 [redacted]

67 [redacted]